MoGua

央行助农钱包 1.0.3.APK 分析报告

APP名称:	央行助农钱包

包名:	com.yhznqb.lmjas
域名线索:	19条
URL线索:	13条
邮箱线索:	2条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 央行助农钱包.apk
文件大小: 67.08MB
MD5值: 2fb5496ca7729c6789f57be0a49a23be
SHA1值: c8f54cf4fa11973b4b55165dd1181674c0f15f5b
SHA256值: af87c1b4a9cf86990b192050f67212b9faa5af67cad581b36b4fb3b6dc20ac88

APP 信息

App名称: 央行助农钱包
包名: com.yhznqb.lmjas
主活动Activity: com.v2ray.ang.ui.SplashActivity
安卓版本名称: 1.0.3
安卓版本: 1003

域名线索

域名	服务器信息
tbs.imtt.qq.com	**IP**: 36.249.65.140 **所属国家**: China **地区**: Fujian **城市**: Quanzhou **纬度**: 24.913891 **经度**: 118.585831
yh.amhsq.org	没有服务器地理信息.
www.google.com	**IP**: 31.13.73.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249

debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
t.me	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
18.163.190.46	**IP**: 18.163.190.46 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
raw.githubusercontent.com	**IP**: 185.199.110.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
log.tbs.qq.com	**IP**: 124.95.231.218 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
plus.google.com	**IP**: 199.16.156.103 **所属国家**: United States of America **地区**: Georgia **城市**: Atlanta **纬度**: 33.770844

	经度: -84.377632
github.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.amazon.com	**IP**: 3.165.85.38 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
10.0.2.2	**IP**: 10.0.2.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
pms.mb.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.gstatic.com	**IP**: 203.208.49.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 60.29.240.17 **所属国家**: China

cfg.imtt.qq.com	**地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mdc.html5.qq.com	**IP**: 116.130.223.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
f-droid.org	**IP**: 104.244.43.231 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
play.google.com	**IP**: 59.24.3.174 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL**信息**	Url**所在文件**

https://plus.google.com/	V/D.java
http://www.amazon.com/gp/mas/dl/android?p=	com/github/javiersantos/appupdater/Config.java
https://f-droid.org/repository/browse/?fdid=	com/github/javiersantos/appupdater/Config.java
https://github.com/	com/github/javiersantos/appupdater/Config.java
https://play.google.com/store/apps/details?id=%s&hl=%s	com/github/javiersantos/appupdater/Config.java
https://play.google.com/store/apps/details?id=	com/github/javiersantos/appupdater/UtilsLibrary.java
https://f-droid.org/repository/browse/?fdid=	com/github/javiersantos/appupdater/UtilsLibrary.java
http://www.amazon.com/gp/mas/dl/android?p=	com/github/javiersantos/appupdater/UtilsLibrary.java
https://github.com/	com/github/javiersantos/appupdater/UtilsLibrary.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java

https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
https://www.gstatic.com/generate_204	com/v2ray/ang/AppConfig.java
https://www.google.com/generate_204	com/v2ray/ang/AppConfig.java
https://github.com/Loyalsoldier/v2ray-rules-dat/releases/latest/download/	com/v2ray/ang/AppConfig.java
http://18.163.190.46:3000/api/nodes/app/R595021	com/v2ray/ang/AppConfig.java
https://t.me/github_2dust	com/v2ray/ang/AppConfig.java
http://18.163.190.46:3000/api/versions/latest/R595021	com/v2ray/ang/AppConfig.java
https://yh.amhsq.org	com/v2ray/ang/AppConfig.java
https://raw.githubusercontent.com/2dust/androidpackagenamelist/master/proxy.txt	com/v2ray/ang/AppConfig.java
https://raw.githubusercontent.com/2dust/v2rayCustomRoutingList/master/	com/v2ray/ang/AppConfig.java
https://github.com/2dust/v2rayNG/issues	com/v2ray/ang/AppConfig.java
https://raw.githubusercontent.com/2dust/v2rayNG/master/CR.md	com/v2ray/ang/AppConfig.java
https://github.com/2dust/v2rayNG	com/v2ray/ang/AppConfig.java
https://github.com/2dust/v2rayNG/wiki/Mode	com/v2ray/ang/AppConfig.java
https://www.google.com	com/v2ray/ang/util/SpeedtestUtil.java

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	i0/AbstractC0263e4.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	h0/w.java
http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	S/j.java
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=央行助农钱包, OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-17 08:11:18+00:00
有效期至: 2050-04-11 08:11:18+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=央行助农钱包, OU=Android, CN=Android
序列号: 0x6829499c6344c1df

哈希算法: sha256
md5值: 789060bad4ef840d296abe47fe869347
sha1值: da1257044ab584161ab0bbae8d1462ec04ea7b4a
sha256值: 62e31e4397ae4226d6975c66df7d84f632b6c1a52f40cb8ed67584417f3d5408
sha512值: 206a3d7e9a56b87c8cfe56c267a544b014ee3f1424792201a9719d578dc2e3db8b143c22505e35f53d6a5a7348376d21b3e17a9f19ebefeba09b3f631e93bfa8
公钥算法: rsa
密钥长度: 2048
指纹: 2325d73a30e93858228fa959c1e0da5f99f5821a6280db487ccfdf29dd7e74ef

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

	是否		

向手机申请的权限	危险	类型	详细情况
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前

android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
com.yhznqb.lmjas.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.v2ray.ang.ui.UrlSchemeActivity	Schemes: v2rayng://, Hosts: install-config, install-sub, Mime Types: text/plain,

---

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。